

## Research Project Experiences

1. On the Security Evaluation of Block Ciphers and their Crypto-Logics : Research Staff Member (Jun/2001 - Nov/2001)
  2. Study on Block Cipher Cryptanalyses: Research Staff Member (Sep/2003 - April/2004)
  3. On the Provable Security for Cryptographic Primitives: Research Staff Member (May/2004 - Feb/2005)
  4. Design of Block Ciphers and Hash Functions Suitable for Ubiquitous System: Research Staff Member (March/2004 - Dec/2005)
  5. Study on Evaluation Algorithms of Hash Functions: Research Staff Member (Main leader) (Feb/2007 - Oct/2007)
  6. Development and Security Analysis of New Hash Algorithms: Research Staff Member (May/2008 - Nov/2008)
  7. Development of Key Schedule for 192-bit and 256-bit key SEED versions: Research Staff Member (Feb/2008 - Nov/2008)
  8. Development of the SHA-3 hash algorithm: NIST Internal Evaluator (Oct/2009 - Present)
  9. Evaluation of AES Key-Wrap Algorithms: NIST Internal Evaluator (Oct/2009 - Present)
  10. Study on Light-weight Algorithms for Constraint Areas: NIST Internal Evaluator (Jan/2011 - Aug/2012)
- 

## Company Project Experiences

1. USB Protocol (Embedded Kernel Level) for IRISYS Co. Ltd. (Jan/2016 - April/2016)
2. Encrypted Messenger for IRISYS Co. Ltd. (April/2016 - June/2016)
3. Automatic Encryption (Embedded Kernel Level) for IRISYS Co. Ltd. (February/2016 - June/2016)
4. FIDO U2F (Embedded Kernel Level) for IRISYS Co. Ltd. (October/2015 - Aug/2016)
5. FIDO UAF (Embedded Kernel Level) for IRISYS Co. Ltd. (July/2016 - November/2016)
6. Design and implementation of Iris Recognition Algorithm for IRISYS Co. Ltd. (Jan/2016 - Aug/2016)
7. Hospital Management (IoT) for Nextronics Co. Ltd. (April/2016 - July/2016)
8. Parking Control with automated billing system (IoT) for Nextronics (April/2016 - July/2016)
9. Traffic Signal Automation (IoT) for Nextronics (April/2016 - September/2016)
10. Verilog Design of Hash Algorithm, Encryption Scheme, BCH code for IRISYS Co. Ltd. (August/2016 - March/2018)
11. CCTV Camera Module Development for Normal IP camera and Thermal Camera (Oct/2016 - Jan/2017)
12. Development of Fingerprint Algorithm for Fuzzy Extractor for ETRI (Electronics and Telecommunications Research Institute) (May/2017 - Oct/2017)
13. Development and integration of Smart Bulb with Alexa services for Merlotlab (Dec/2017 - March/2018)

14. FIDO2 CTAP Protocol (Embedded Kernel Level) for ETRI (May/2018 - Nov/2018)
15. Development of Multi-lane Detection Algorithm using Deep learning for SpringCloud Co. Ltd. (July/2018 - Dec/2018)
16. Development of Spoofing Detection Algorithm for Iris and Face recognition System for IRISYS Co. Ltd. (Feb/2018 - Present)